



HF 2PW

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re patent application of:	) Date: August 18, 2004
Perry A. Pierce	) Attorney Docket No.: E-925
Serial No.: 09/475,912	) Customer No.: 00919
Filed: December 30, 1999	) Group Art Unit: 3625
Confirmation No.: 7042	) Examiner: James H. Zurita
Title:	<b>METHOD AND SYSTEM FOR DATA REPOSITORY</b>

**TRANSMITTAL OF APPEAL BRIEF (PATENT APPLICATION 37 CFR 1.192)**

Mail Stop Appeal Brief-Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Transmitted herewith in **triplicate** is the **APPEAL BRIEF** in the above-identified patent application with respect to the Notice of Appeal filed on June 21, 2004.

The filing fee was paid in connection with the Appeal Brief filed June 2, 2003. No additional filing fees are required herewith for the filing of the within Appeal Brief.



- 2 -

A duplicate copy of this transmittal is enclosed for use in charging the Deposit Account.

Respectfully submitted,

Ronald Reichman  
Reg. No. 26,796  
Attorney of Record  
Telephone (203) 924-3854

PITNEY BOWES INC.  
Intellectual Property and  
Technology Law Department  
35 Waterview Drive  
P.O. Box 3000  
Shelton, CT 06484-8000

#### CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

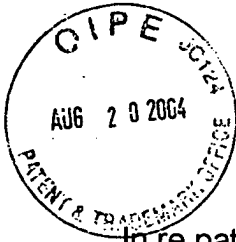
Mail Stop Appeal Brief-Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

On August 18, 2004  
Date of Deposit

Esther A. Lapin  
Name of Rep.

  
Signature

August 18, 2004  
Date



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re patent application of:

) Attorney Docket No.: E-925

Perry A. Pierce

) Group Art Unit: 3625

Serial No.: 09/475,912

) Examiner: James H. Zurita

Filed: December 30, 1999

) Date: August 18, 2004

Confirmation No.: 7042

) Customer No.: 00919

Title: **METHOD AND SYSTEM FOR DATA REPOSITORY**

**APPELLANT'S BRIEF**

Mail Stop Appeal Brief - Patent  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This Brief is in furtherance of the Notice of Appeal filed in this case on June 21, 2004.

This Brief is transmitted in triplicate.

## **TABLE OF CONTENTS**

This Brief contains these items under the following headings and in the order set forth below.

- I. REAL PARTY IN INTEREST
- II. RELATED APPEALS AND INTERFERENCES
- III. STATUS OF CLAIMS
- IV. STATUS OF AMENDMENTS
- V. SUMMARY OF INVENTION
- VI. ISSUES PRESENTED FOR REVIEW
- VII. GROUPINGS OF CLAIMS
- VIII. ARGUMENTS
- IX. PRAYER FOR RELIEF
- X. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

## **I. REAL PARTY IN INTEREST**

Pitney Bowes Inc. is the real party in interest.

## **II. RELATED APPEALS AND INTERFERENCES**

There are no related Appeals and interferences

## **III. STATUS OF CLAIMS**

- a) Claims 1, 3 – 7, 9 –17 and 19 - 24 are in the application.
- b) Claims 1, 3 – 7, 9 –17 and 19 - 24 are rejected
- d) Claims 1, 3 – 7, 9 –17 and 19 - 24 are on appeal

## **IV. STATUS OF AMENDMENTS**

An Amendment subsequent to the Final Rejection of March 22, 2004, was filed on May 3, 2004. This Amendment was not entered.

## **V. SUMMARY OF THE INVENTION**

### **A. Background**

The prior art did not provide for electronically selling a data item that is stored by a seller in a repository, wherein the fee for downloading the data item is in a range specified by the seller and defined by a maximum amount posted by the seller, and a minimum amount that the seller is willing to collect from the buyer so that the buyer is allowed to download the data item if the buyer's proposed monetary sum for downloading the data item is greater or equal to the

**minimum amount specified by the seller and to provide a digital signature to the buyer to verify the authenticity of the downloaded data item through a certification authority.**

It is well known that a data item such as a song, a piece of music, a document, a legal form, a book, a research report or a picture can be purchased through the Internet. Currently, there are two widely used methods for making such a transaction electronically.

One current method is for the seller to send the data item directly to the buyer via e-mail, wherein the price for buying the data item is negotiated between the two parties and the money is sent to the seller according to a paying method agreed upon. The major shortcoming of this method is that the seller must know the buyer or have faith in the buyer, hoping that the buyer will eventually pay for the data item. Furthermore, when the data item is sold to a large number of buyers, the seller must set up a system to keep track of which buyers have paid and which buyers have not yet paid. Many sellers may not have the temperament, the knowledge or the time to tend to the administrative aspect of doing business.

The other current method is for the seller to upload the data item to an Internet service provider or a Web site operator. The Internet service provider/Web site operator will then notify the buyer via e-mail with a unique universal resource locator (URL) to allow the buyer to download the data item through the URL. Musical works have been purchased in this fashion wherein a buyer can download a song in an MP3 file to the buyer's computer. With this method, however, the buyer must provide a credit card number to be charged for downloading the data item. This is not advantageous to the

Internet service provider/Web site operator who provides the transaction service because credit card and bank fees are typically larger with high volume, low amount transactions.

**B. Appellant claims a system and method that provides for electronically selling a data item that is stored by a seller in a repository, wherein the fee for downloading the data item is in a range specified by the seller and defined by a maximum amount posted by the seller, and a minimum amount that the seller is willing to collect from the buyer so that the buyer is allowed to download the data item if the buyer's proposed monetary sum for downloading the data item is greater or equal to the minimum amount specified by the seller and to provide a digital signature to the buyer to verify the authenticity of the downloaded data item through a certification authority.**

The present invention provides a method and system for electronically selling a data item such as a song, a literature piece or a picture. A data repository is used for a seller to store the data item that the seller wishes to sell for a fee. The data repository is accessible to a buyer who deposits a fund to the data repository prior to downloading the data item. The data repository is connected to a telecommunication network such as the Internet so that the buyer can download the purchased data item directly through the telecommunication network. The seller posts a price that is the maximum amount the seller wishes to collect, and sets a minimum amount that the seller is willing to collect from the buyer for downloading the data item. The buyer makes an offer to the

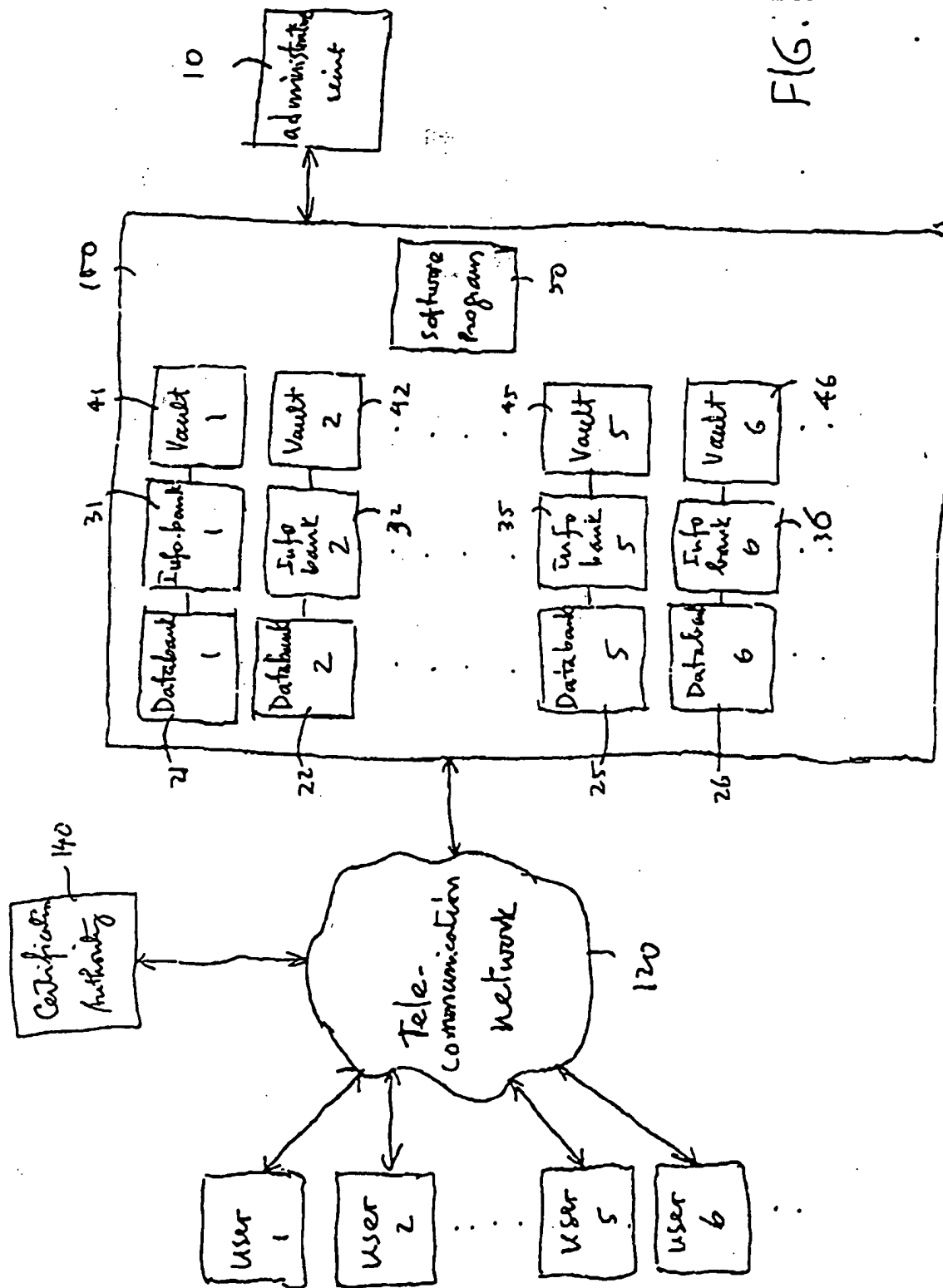


FIG. 1



data repository wherein a software program is used to determine if offered price falls within the fee range as set by the seller.

As shown in Fig. 1 and pages 6 and 7 of Appellant's specification, the data repository system **100** includes a plurality of data banks (**21-26**), a plurality of information banks (**31-36**), a plurality of electronic vaults (**41-46**), and a software program **50**. The data repository system **100** allows access by a plurality of users (**11-16**). Also shown in Figure 1 is an administrative unit **10** that manages the data repository system **100**. It is understood that the data bank **21**, the information bank **31** and the vault **41** are associated with the user **11**, for example. The data bank can be used by the user **11** to store one or more data items that the user **11** wishes to sell electronically for a fee. However, the data bank **21** can also be used for the user **11** to download a data item from other data banks (**22-26**) if the user **11** pays a fee for downloading the data item. Thus, any user can be a seller or a buyer or both. Accordingly, the vault **41** can be used for storing proceeds from selling a data item that are credited to the seller, but it can also be used for depositing a fund so as to allow a buyer to use part or all of the fund to pay for downloading one or more data items.

Preferably, the data repository system **100** is connected to a telecommunication network **120**, such as the Internet, so as to allow the users (**11-16**) to access the data repository system **100** through the telecommunication network **120**. Preferably, a Certification Authority **140** is also connected through the telecommunication network **120** so as to allow the buyer to verify the authenticity of the downloaded data items. Preferably, the Certification Authority **140** is provided by a third party who is independent of the users (**11-16**) and the data repository system **100**.

Preferably, the software program **50** has an encryption function to encrypt a data item prior to said data item being conveyed to the buyer through the telecommunication network **120**. The encryption is used to prevent the conveyed data item being intercepted by an unauthorized person who may use the data item without paying a fee to the seller.

To download a data item, the buyer must deposit a fund which must be sufficient to pay for downloading the data item. The fund can be a monetary sum deposited to a bank designated by the service provider of the data repository, or a bank account provided by the buyer where money can be withdrawn for paying the data item. The fund can also be in the form of a debit card, a smartcard or a stored-value card.

## **VI. ISSUES PRESENTED FOR REVIEW**

1. Whether or not claims 1 and 17 are patentable under 35 USC §101.
2. Whether or not claims 1 and 17 are patentable under 35 USC §112 for failing to comply with the written description requirement.
3. Whether or not claims 1 and 17 are patentable under 35 USC §112 for failing to particularly point out and distinctly claim the subject matter that Appellant regards as the invention.
  - A. Whether or not claims 1, 3, 4, 6, 7, 9, 16, 17, 19, 23 and 24 are patentable under 35 USC §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).
  - B. Whether or not claim 5 is patentable under 35 USC §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).

- C. Whether or not claim 10 is patentable under 35 USC §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).
- D. Whether or not claim 11 is patentable under 35 USC §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).
- E. Whether or not claim 12 is patentable under 35 USC §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).
- F. Whether or not claim 13 is patentable under 35 USC §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).
- G. Whether or not claims 14, 15, 21 and 22 are patentable under 35 USC §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).
- H. Whether or not claim 20 is patentable under 35 USC §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).

## **VII. GROUPING OF CLAIMS**

- A. Claims 1, 3, 4, 6, 7, 9, 16, 17, 19, 23 and 24 stand or fall together with regard to the rejection under 35 U.S.C. §103(a).
- B. Claim 5 stands or falls with regard to the rejection under 35 U.S.C. §103(a).
  - C. Claim 10 stands or falls with regard to the rejection under 35 U.S.C. §103(a).
  - D. Claim 11 stands or falls with regard to the rejection under 35 U.S.C. §103(a).
  - E. Claim 12 stands or falls with regard to the rejection under 35 U.S.C. §103(a).

- F. Claim 13 stands or falls with regard to the rejection under 35 U.S.C. §103(a).
- G. Claims 14, 15, 21 and 22 stand or fall together with regard to the rejection under 35 U.S.C. §103(a).
- H. Claim 20 stands or falls with regard to the rejection under 35 U.S.C. §103(a).

## **VIII. ARGUMENTS**

- 1. Claims 1 and 17 have been rejected by the Examiner under U.S.C. §101 because the disclosed invention is inoperative and therefore lacks utility.**

The Examiner under 35 USC §101 has rejected claims 1 and 17, because in the Examiner's opinion the disclosed invention is inoperative and, therefore, lacks utility. In the Examiner's opinion, Claim 1 is inoperative since no processor was claimed to run the claimed program. Claim 1 is not inoperative as the function of a processor is claimed in the following portion of claim 1.(c)(ii), which reads as follows:

"(ii) the information storage is for posting the fee for downloading the data item from the data storage, and the buyer deposits the fund in the monetary storage prior to downloading the data item; wherein said data repository system further comprises a program capable of communicating with the data storage, the information storage and the monetary storage so as to store a fund deposited by the buyer to pay for downloading the data item into the buyer's account;"

Claim 17 is not inoperative since the function of a processor is claimed in the following portion of claim 17 c)

"downloading a portion of the data item so that the buyer may review a portion of the data item without the possibility of downloading the entire data item without paying the seller; "

In the Examiner's opinion, claims 1 and 17 claim functions that Appellant ascribed to digital signatures when the digital signatures are carried out by digital certificates. The definition used by the Examiner in the March 22, 2004, Final Rejection is only one of the various methods used to perform secure communications using digital signatures and certificates.

The description given by Appellant in lines 20-38 of page 6 and lines 15-20 of page 8 of Appellant's specification define the method used by Appellant to perform secure communication using digital signatures and digital certificates.

Lines 20-28 of page 6 of Appellant's specification read as follows:

"Preferably, the data repository system **100** is connected to a telecommunication network **120**, such as the Internet, so as to allow the users (**11-16**) to access the data repository system **100** through the telecommunication network **120**. Preferably, a Certification Authority **140** is also connected through the telecommunication network **120** so as to allow the buyer to verify the authenticity of the downloaded data items. Preferably, the Certification Authority **140** is provided by a third party who is independent of the users (**11-16**) and the data repository system **100**."

Lines 15-20 of page 8 of Appellant's specification read as follows:

"Preferably, a digital signature of the seller is also stored in the identification code storage area **312** so that the digital signature can be provided to the buyer when the buyer downloads the data item. With the digital signature, the buyer can verify the authenticity of the downloaded data

item. Similarly, a buyer may use his/her password to access the associated vault to check the balance.”

Claim 1(c)(vii) and (viii) read as follows:

“(vii) to encrypt the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and

(viii) to provide a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.”

Subdivisions (g) and (f) of claim 17 reads as follows:

“f) encrypting the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and

g) providing a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.”

Subdivision (c)(vii) of claim 1 and (f) of claim 17 is done so that any thing being downloaded will happen over a secure connection. Subdivision (c)(viii) of claim 1 and subdivision (g) of claim 17 allows an author A to place to a digital signature on this proprietary item that is being downloaded so that user U can authenticate the validity of the downloaded item. For instance, author A posts content with a digital signature, user U downloads author A's content from source S and validates the content using A's digital signature. In the foregoing manner, user U is sure he/she obtained author A's content and not the content prepared by a party other than author A.

The method used by Appellant as set forth in the specification to perform secure communications using digital signatures and digital certificates is also described in

pages 571 and 572 of *Applied Cryptography, Second Edition* by Bruce Schneier, published by John Wiley & Sons, Inc., 1996, which reads as follows:

#### **"24.6 KryptoKnight**

KryptoKnight (Kryptonite - get it?) is an authentication and key distribution system designed by IBM. It is a secret-key protocol and uses either DES in CBC mode (see Section 9.3) or a modified version of MD5 (see Section 18.5).

KryptoKnight supports four security services:

- User authentication (called single sign-on)
- Two-party authentication
- Key distribution
- Authentication of data origin and content"

Furthermore, the Examiner is not following the spirit of MPEP §2106 II when he does not reject essentially the same claim under 35 USC §101 in four prior patent office substantive actions, i.e., April 23, 2002; August 16, 2002; January 13, 2003; and September 9, 2003; and rejects this claim under 35 USC §101 in the fifth substantive office action of March 22, 2004.

MPEP §2106 II reads as follows:

#### **"II. DETERMINE WHAT APPELLANT HAS INVENTED AND IS SEEKING TO PATENT**

It is essential that patent applicants obtain a prompt yet complete examination of their applications. Under the principles of compact prosecution, each claim should be reviewed for compliance with every statutory requirement for patentability in the initial review of the application, even if one or more claims are found to be deficient with respect to some statutory requirement. Thus, Office personnel should state all reasons and bases for rejecting claims in the first Office action. Deficiencies should be explained clearly, particularly when they serve as a basis for a rejection. Whenever practicable, Office personnel should indicate how rejections may be overcome and how problems may be resolved. A failure to follow this approach can lead to unnecessary delays in the prosecution of the application."

**2. Claims 1 and 17 have been rejected by the Examiner under U.S.C. §112 for failing to comply with the written description requirement.**

Claims 1, 17 and those claims dependent thereon have been rejected by the Examiner under 35 USC §112 for failing to comply with the written description requirement. The Examiner is of the opinion subdivision (c)(viii) of claim 1 to provide a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certificate authority and subdivision (g) of claim 17, providing a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority fails to comply with the written description requirement of 35 USC §112.

The description given by Appellant in line 20 of page 6 to line 4 of page 7 and lines 15-21 of page 8 of Appellant's specification supply the needed written description.

**3. Claims 1 and 17 are have been rejected by the Examiner under 35 USC §112 for failing to particularly point out and distinctly claim the subject matter that Appellant regards as the invention.**

The Examiner rejected claims 1 and 17 and those claims dependent thereon under 35 USC §112 as being indefinite for failing to particularly point out and claim the subject matter which Appellant regards as the invention. The claims refer to providing a digital signature to a buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority, i.e., claim 1, (c) (viii) to provide a



digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority, and claim 17 (g) i.e., g) providing a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.

The Examiner is also of the opinion that, where Appellant acts as his/her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the Appellant intended to so redefine that claim term.

Appellant specifically defined the terms in line 20 of page 6 to line 4 of page 7 of Appellant's specification, which reads as follows:

"Accordingly, the vault **41** can be used for storing proceeds from selling a data item that are credited to the seller, but it can also be used for depositing a fund so as to allow a buyer to use part or all of the fund to pay for downloading one or more data items.

Preferably, the data repository system **100** is connected to a telecommunication network **120**, such as the Internet, so as to allow the users (**11-16**) to access the data repository system **100** through the telecommunication network **120**. Preferably, a Certification Authority **140** is also connected through the telecommunication network **120** so as to allow the buyer to verify the authenticity of the downloaded data items. Preferably, the Certification Authority **140** is provided by a third party who is independent of the users (**11-16**) and the data repository system **100**."

and lines 15-21 of page 8 of Appellant's specification, which reads as follows:

"The identification code storage area **312** is used to store a unique code, such as a password, provided by or assigned to a user in order for the user to access the data bank, the information bank or the vault associated with the user. For example, a seller may use his/her password to access the associated data bank to modify the data item, to access the transaction record to review the statistics,

or to access the vault to check on the accumulated proceeds or to transfer the money out of the vault.”

The method used by Appellant as set forth in the above portion of the specification to perform secure communications using digital signatures and digital certificates is also described in pages 571 and 572 of *Applied Cryptography, Second Edition* by Bruce Schneier, published by John Wiley & Sons, Inc., 1996, which reads as follows:

#### **“24.6 KryptoKnight**

KryptoKnight (Kryptonite - get it?) is an authentication and key distribution system designed by IBM. It is a secret-key protocol and uses either DES in CBC mode (see Section 9.3) or a modified version of MD5 (see Section 18.5).

KryptoKnight supports four security services:

- User authentication (called single sign-on)
- Two-party authentication
- Key distribution
- Authentication of data origin and content”

Thus, Appellant has used terms that are recognized in the art and particularly pointed out and claimed the subject matter which Appellant regards as the invention.

**A. Claims 1, 3, 4, 6, 7, 9,16, 17, 19, 23 and 24 have been rejected by the Examiner under 35 USC §103(a) as being unpatentable over Ginter, et al. (U.S. Patent No. 5,892,900).**

Ginter discloses the following in line 66 of column 270 to line 36 of column 271.

“A more complex form of negotiation is analogous to “haggling.” In this scenario, most of the terms and conditions are fixed, but one or more terms (e.g., price or payment terms) are not. For these terms, there are options, limits and elements that may be negotiated over. A VDE electronic negotiation between two

parties may be used to resolve the desired, permitted, and optional terms. The result of the electronic negotiation may be a finalized set of rules and control information that specify a completed electronic contract. A simple example is the scenario for purchasing software described above adding the ability of the purchaser to select a method of payment (VISA, MasterCard, or American Express). A more complex example is a scenario for purchasing information in which the price paid depends on the amount of information about the user that is returned along with a usage audit trail. In this second example, the right to use the content may be associated with two control sets. One control set may describe a fixed ("higher") price for using the content. Another control set may describe a fixed ("lower") price for using the content with additional control information and field specifications requiring collection and return the user's personal information. In both of these cases, the optional and permitted fields and control sets in a PERC may describe the options that may be selected as part of the negotiation. To perform the negotiation, one party may propose a control set containing specific fields, control information, and limits as specified by a PERC; the other party may pick and accept from the control sets proposed, reject them, or propose alternate control sets that might be used. The negotiation process may use the permitted, required, and optional designations in the PERC to determine an acceptable range of parameters for the final rule set. Once an agreement is reached, the negotiation process may create a new PERC and/or URT that describes the result of the negotiation. The resulting PERCs and/or URTs may be "signed" (e.g., using digital signatures) by all of the negotiation processes involved in the negotiation to prevent repudiation of the agreement at a later date."

Ginter discloses the following in line 56 of column 127 to line 3 of column 128.

"SE 503/HPE 655 may support both Public Key type keys and Bulk Encryption type keys. The public key (PK) encryption type keys stored by SPU 500 and managed by key and tag manager 558 may include, for example, a device public key, a device private key, a PK certificate, and a public key for the certificate. Generally, public keys and certificates can be stored externally in non-secured memory if desired, but the device private key and the public key for the certificate should only be stored internally in an SPU 500 EEPROM or NVRAM 534b. Some of the types of bulk encryption keys used by the SPU 500 may include, for example, general purpose bulk encryption keys,

administrative object private header keys, stationary object private header keys, traveling object private header keys, download/initialization keys, backup keys, trial keys, and management file keys.”

Ginter discloses the following in line 39 of column 211 to line 24 of column 212.

“In the preferred embodiment, PPE 650 may generate its own certificate, or the certificate may be obtained externally, such as from a certifying authority VDE administrator. Irrespective of where the digital certificate is generated, the certificate is eventually registered by the VDE administrator certifying authority so that other VDE electronic appliances 600 may have access to (and trust) the public key. For example, PPE 650 may communicate its public key and other information to a certifying authority which may then encrypt the public key and other information using the certifying authority’s private key. Other installations 600 may trust the “certificate” because it can be authenticated by using the certifying authority’s public key to decrypt it. As another example, the certifying authority may encrypt the public key it receives from the generating PPE 650 and use it to encrypt the certifying authority’s private key. The certifying authority may then send this encrypted information back to the generating PPE 650. The generating PPE 650 may then use the certifying authority’s private key to internally create a digital certificate, after which it may destroy its copy of the certifying authority’s private key. The generating PPE 650 may then send out its digital certificate to be stored in a certification repository at the VDE administrator (or elsewhere()) if desired. The certificate process can also be implemented with an external key pair generator and certificate generator, but might be somewhat less secure depending on the nature of the secure facility. In such a case, a manufacturing key should be used in PPE 650 to limit exposure to the other keys involved.

A PPE 650 may need more than one certificate. For example, a certificate may be needed to assure other users that a PPE is authentic, and to identify the PPE. Further certificates may be needed for individual users of a PPE 650. These certificates may incorporate both user and site information or may only include user information. Generally, a certifying authority will require a valid site certificate to be presented prior to creating a certificate for a given user. Users may each require their own public key/private key pair in order to obtain certificates. VDE administrators, clearinghouses, and other participants may normally require authentication of both the site (PPE 650) and

of the user in a communication or other interaction. The processes described above for key generation and certification for PPEs 650 may also be used to form site/user certificates or user certifications.

Certificates as described above may also be used to certify the origin of load modules 1100 and/or the authenticity of administrative operations. The security and assurance techniques described above may be employed to decrease the probability of compromise for any such certificate (including certificates other than the certificate for a VDE electronic appliance 600's identity)."

Ginter does not disclose or anticipate paragraphs (vi), (vii), and (viii) of claim 1 as amended, and those claims dependent thereon, namely, to credit the monetary sum to the seller's account, wherein the fee for downloading the data item has a range specified by the Seller and defined by a maximum amount, and a minimum amount wherein the maximum amount is the fee posted by the Seller, and a minimum amount is what the Seller is willing to collect from the buyer for downloading the data item so that the buyer is allowed to download the data item if the buyer's proposed monetary sum for downloading the data item is greater or equal to the minimum amount specified by the seller and after the buyer's proposed monetary sum is deducted from the buyer's account and credited to the seller's account; to encrypt the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and to provide a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.

Ginter also does not disclose or anticipate steps e), f), and g) of claim 17 as amended and those claims dependent thereon, namely, deducting a monetary sum from the fund and crediting the deducted sum to the seller, wherein the fee for

downloading the data item in its entirety has a range specified by the Seller and defined by a maximum amount, and a minimum amount wherein the maximum amount is the fee posted by the Seller, and a minimum amount is what the Seller is willing to collect from the buyer for downloading the data item so that the buyer is allowed to download the data item if the buyer's proposed monetary sum for downloading the data item is greater or equal to the minimum amount specified by the seller; encrypting the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and providing a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.

Ginter does not disclose or anticipate a scenario in which the seller may say he/she wants \$1.00 for the item, and the buyer may propose \$.85. If the \$.85 is within the seller's range, the item is purchased. However, if the \$.85 is not within the seller's range, the item is not purchased.

Ginter uses a fixed ("higher") price for using the content and another fixed ("lower") price for using the content with additional control information and field specifications requiring collection and return the user's personal information. Ginter does not automatically check the offered price by the buyer to determine whether the posted offer falls within the range specified by the seller.

Ginter does not to encrypt the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and provide a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.

**B. Claim 5 has been rejected by the Examiner under U.S.C. §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).**

In dependent claim 5, the seller pays a commission for selling the item to the buyer and the commission is deducted from the fee credited to the seller.

In addition to the arguments made in above Section A, the cited references do not disclose or anticipate a user fee or commission that is deducted from the fee credited to the seller.

**C. Claim 10 has been rejected by the Examiner under U.S.C. §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).**

In dependent claim 10, the seller uses an identification code to modify the data item and/or the fee.

In addition to the arguments made in above Section A, the cited references do not disclose or anticipate using an identification code to modify the data item and/or the fee.

**D. Claim 11 has been rejected by the Examiner under U.S.C. §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).**

In dependent claim 11, the data storage further stores an excerpt of the data item so as to allow the buyer to review the data item without the possibility of downloading the data item without paying the seller.

In addition to the arguments made in above Section A, the cited references do not disclose or anticipate storing an excerpt of the data item so as to allow the buyer to

review the data item without the possibility of downloading the data item without paying the seller.

**E. Claim 12 has been rejected by the Examiner under U.S.C. §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).**

In dependent claim 12, an administrative unit is used for notifying a user of the data repository system of problems related to the use of the data repository system.

In addition to the arguments made in above Section A, the cited references do not disclose or anticipate using an administrative unit for notifying a user of the data repository system of problems related to the use of the data repository system.

**F. Claim 13 has been rejected by the Examiner under U.S.C. §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).**

In dependent claim 13, the data storage includes a plurality of data banks each of which is used to store a data item and an excerpt of said data item.

In addition to the arguments made in above Section A, the cited references do not disclose or anticipate a data storage that includes a plurality of data banks each of which is used to store a data item and an excerpt of said data item.

**G. Claims 14, 15, 21, and 22 have been rejected by the Examiner under U.S.C. §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).**



In dependent claims 14 and 21, the fund is deposited in a bank, and the deposited fund can be withdrawn by the data repository system to pay for downloading the data item.

In dependent claims 15 and 22, the fund is stored in a stored-value card and the stored fund can be withdrawn by the data repository system to pay for downloading the data item.

In addition to the arguments made in above Section A, the cited references do not disclose or anticipate the fund is stored or deposited and the stored or deposited fund can be withdrawn by the data repository system to pay for downloading the data item.

**H. Claim 20 has been rejected by the Examiner under U.S.C. §103(a) over Ginter, et al. (U.S. Patent No. 5,892,900).**

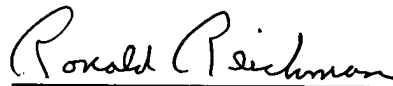
In dependent claim 20, an excerpt of the data item is used for the buyer to review the data item before downloading the data item, said method further comprising the step of downloading an electronic file containing the excerpt to the buyer.

In addition to the arguments made in above Section A, the cited references do not disclose or anticipate an excerpt of the data item that is used by the buyer to review the data item before downloading the data item, said method further comprising the step of downloading an electronic file containing the excerpt to the buyer.

## IX PRAYER FOR RELIEF

Appellant respectfully submits that appealed claims 1, 3 – 7, 9 – 17 and 19 - 24 in this application are patentable. It is requested that the Board of Appeal overrule the Examiner and direct allowance of the rejected claims.

Respectfully submitted,



---

Ronald Reichman  
Reg. No. 26,796  
Attorney of Record  
Telephone (203) 924-3854

PITNEY BOWES INC.  
Intellectual Property and  
Technology Law Department  
35 Waterview Drive  
P.O. Box 3000  
Shelton, CT 06484-8000

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Appeal Brief - Patent  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

On August 18, 2004  
Date of Deposit

Esther A. Lapin  
Name of Rep.

\_\_\_\_\_  
Signature

August 18, 2004  
Date

## **APPENDIX OF CLAIMS**

1. A data repository system to allow a seller to store a data item that the seller wishes to sell electronically to a buyer for a fee, said repository system comprising:
  - a) a data storage;
  - b) an information storage; and
  - c) a monetary storage having a seller's account and a buyer's account, wherein
    - (i) the data storage is used to store the data item; and
    - (ii) the information storage is for posting the fee for downloading the data item from the data storage, and the buyer deposits the fund in the monetary storage prior to downloading the data item; wherein said data repository system further comprises a program capable of communicating with the data storage, the information storage and the monetary storage so as to store a fund deposited by the buyer to pay for downloading the data item into the buyer's account;
    - (iii) to allow the buyer to download a portion of the data item so that the buyer may review the data item without the possibility of downloading the data item in its entirety without paying the seller;
    - (iv) to deduct a monetary sum from the deposited fund according the posted fee in the information storage;
    - (v) to allow the buyer to download the data item from the data storage;
    - (vi) to credit the monetary sum to the seller's account, wherein the fee for downloading the data item has a range specified by the Seller and defined by

a maximum amount, and a minimum amount wherein the maximum amount is the fee posted by the Seller, and a minimum amount is what the Seller is willing to collect from the buyer for downloading the data item so that the buyer is allowed to download the data item if the buyer's proposed monetary sum for downloading the data item is greater or equal to the minimum amount specified by the seller and after the buyer's proposed monetary sum is deducted from the buyer's account and credited to the seller's account;

(vii) to encrypt the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and

(viii) to provide a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.

3. The data repository system of claim 1, wherein the fee deducted from the fund deposited by the buyer is credited to the seller.
4. The data repository system of claim 3, wherein the seller pays a user fee for using the data repository and the user fee is deducted from the fee credited to the seller.
5. The data repository system of claim 3, wherein the seller pays a commission for selling the item to the buyer and the commission is deducted from the fee credited to the seller.

6. The data repository system of claim 3, wherein the monetary storage includes an account for the seller to store the fee credited to the seller.
7. The data repository system of claim 6, wherein the seller uses an identification code to access the seller's account.
9. The data repository system of claim 1, further comprising a software program to automatically check the offered price by the buyer in order to determine whether the posted offer falls within the fee range as specified by the seller.
10. The data repository system of claim 1, wherein the seller uses an identification code to modify the data item and/or the fee.
11. The data repository system of claim 1, wherein the data storage further stores an excerpt of the data item so as to allow the buyer to review the data item without the possibility of downloading the data item without paying the seller.
12. The data repository system of claim 1, further comprising an administrative unit for notifying a user of the data repository system of problems related to the use of the data repository system.

13. The data repository system of claim 1, wherein the data storage includes a plurality of data banks each of which is used to store a data item and an excerpt of said data item.
14. The data repository system of claim 1, wherein the fund is deposited in a bank and the deposited fund can be withdrawn by the data repository system to pay for downloading the data item.
15. The data repository system of claim 1, wherein the fund is stored in a stored-value card and the stored fund can be withdrawn by the data repository system to pay for downloading the data item.
16. The data repository system of claim 1, wherein the data item is encrypted prior to the buyer downloading the data item.
17. A method of providing a service by a service provider to allow a seller to electronically sell a data item for a fee to a buyer who downloads the data item through a telecommunication network, said method comprising the steps of:
  - a) storing the data item in a data repository;
  - b) depositing a fund in the data repository;
  - c) downloading a portion of the data item so that the buyer may review a portion of the data item without the possibility of downloading the entire data item without paying the seller;

- d) downloading the data item from the repository;
  - e) deducting a monetary sum from the fund and crediting the deducted sum to the seller, wherein the fee for downloading the data item in its entirety has a range specified by the Seller and defined by a maximum amount, and a minimum amount wherein the maximum amount is the fee posted by the Seller, and a minimum amount is what the Seller is willing to collect from the buyer for downloading the data item so that the buyer is allowed to download the data item if the buyer's proposed monetary sum for downloading the data item is greater or equal to the minimum amount specified by the seller
  - f) encrypting the data item prior to downloading the data item to the buyer to prevent an unauthorized person from obtaining the downloaded data item by interception; and
  - g) providing a digital signature to the buyer to allow the buyer to verify the authenticity of the downloaded data item through a certification authority.
19. The method of claim 17, wherein the monetary sum is equal to a price offered by the buyer to pay for downloading the data item, said method further comprising the steps of:
- (a) comparing the offered price in order to determine whether the offered price falls within the fee range as specified by the seller.
20. The method of claim 19, wherein an excerpt of the data item is used for the buyer to review the data item before downloading the data item, said method further



comprising the step of downloading an electronic file containing the excerpt to the buyer.

21. The method of claim 17, wherein the fund is deposited in a bank and wherein the deposited fund can be withdrawn into the data repository in order to pay the seller.
22. The method of claim 17, wherein the fund is stored in a stored-value card and wherein the stored fund can be withdrawn into the data repository in order to pay the seller.
23. The method of claim 17 further comprising the step of providing a digital signature when the data item is downloaded from the data repository so as to allow the buyer to verify the authenticity of the downloaded data item.
24. The method of claim 23, wherein the authenticity of the downloaded data item is verified through a Certification Authority.